



電子書

全方位終端安全策略的 5 個基本要素

數位轉型需要以全新視角看待終端安全性

今日的數位勞動力與五年前已經大相逕庭。員工和承包商分佈於多個辦公室及地區。有些員工在家中或共享工作空間內工作。大多數員工使用各種裝置及雲端應用程式完成其工作。

以往清晰明確的網路邊界，因雲端興起而模糊，令您的企業面臨日益複雜且破壞性極大的網路攻擊威脅。未獲得充份保護的桌上型電腦、筆電（甚至 macOS!）及伺服器都會為攻擊者提供竊取資料及破壞的切入點。

網路釣魚和勒索軟體等終端攻擊可能使您的業務中斷，毀損您公司的聲譽並引發訴訟或罰款。事實上，終端攻擊可讓大型企業蒙受平均 700 萬美元的損失，或每台被滲透的裝置須付出約 440 美元的代價。¹ 難怪在 CyberArk 最近對 1,000 名 IT 安全決策者

所做的調查中，60% 的受訪者將外部攻擊（如網路釣魚）列入其最大安全風險清單，59% 受訪者的清單包含勒索軟體。²

資安長及 IT 領導者都對終端安全採取縱深防禦作為反擊策略，以減少暴露風險。本電子書將探討為您的數位業務實行全方位終端安全策略的五個基本要素。多層終端安全計劃可協助您補強安全漏洞、改善安全態勢並降低風險。

一次終端攻擊造成的平均經濟損失超過 700 萬美元¹

¹ 2018 年 Ponemon Institute 終端安全風險現狀

² CyberArk 全球進階威脅形勢 2019 年報告

縱深防禦終端安全策略

預防多種威脅

數位轉型為安全、合規及風險管理專業人員帶來各種挑戰。現今的數位業務面臨各式各樣的威脅 – 從重創企業的勒索軟體攻擊至代價高昂的資料外洩。惡意攻擊者、網路犯罪份子、甚至不懷好意的競爭對手都可利用隨時可用的開放原始碼工具取得終端的存取權，並侵入您的網路以竊取機密資訊或干擾服務。

具有前瞻性思維的企業組織會對終端安全採取縱深防禦做法、建立各種安全控制措施來預防各種威脅。縱深防禦方法的構想最初來自美國國家安全局，採用多層次的安全措施消弭漏洞、減少攻擊面及遏制風險。



終端

名詞

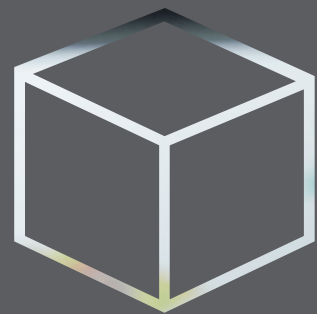
任何可藉以進入公司資產及應用程式的裝置，是潛在的資安漏洞。終端包括桌上型電腦、筆記型電腦及伺服器。



終端安全策略的 五個基本要素

全方位的終端安全策略包括五個基本要素：

- ▣ 終端偵測及回應（EDR）工具
- ▣ 防病毒及下一代防病毒保護工具
- ▣ 特權管理解決方案
- ▣ 應用程式修補工具及最佳實踐解決方案
- ▣ 作業系統修補工具及最佳實踐做法



終端偵測及回應

偵測及回應終端上的
進階主動攻擊

要素一： 終端偵測及回應工具

終端偵測及回應工具可讓您主動識別及調查終端上的可疑活動。大多數 EDR 解決方案都會持續監控、記錄及分析終端活動，協助 IT 和專業安全人員有效發現及減少進階威脅。

[Gartner](#) 指出，EDR 解決方案具備下列能力：

- 偵測安全事件
- 遏制終端上的事件
- 調查安全事件
- 提供修復指引

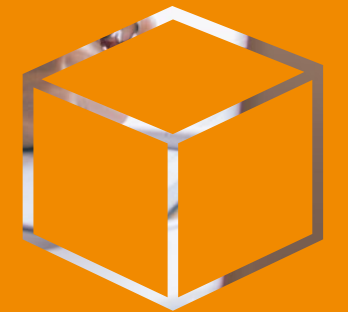
許多 EDR 解決方案使用進階分析技術分析終端事件，以偵測可能未被察覺的惡意活動。EDR 工具可即時檢視可疑終端的行為，協助您在威脅紮根並傳播至整個企業之前攔阻下來。

要素二： 防病毒及下一代防病毒保護工具

防病毒（AV）及下一代防病毒（NGAV）保護工具可協助您偵測及移除各種形式的惡意軟體。傳統的防病毒解決方案透過檢查檔案及尋找已知病毒的特徵碼來識別及防堵惡意程式。傳統防病毒工具雖然在引入初時很有效，卻無法偵測到更新型的威脅，例如無檔案惡意軟體和零時差攻擊等。事實上在一項 Ponemon Institute 調查中，62% 的受訪者表示他們的傳統防病毒解決方案只能減少 50% 或以下的攻擊。³

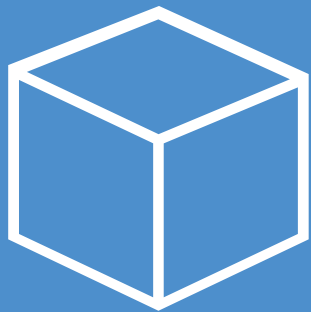
下一代防病毒保護解決方案利用預測分析、人工智慧（AI）及機器學習（ML）來防禦現代攻擊，例如可躲避傳統防病毒程式的勒索軟體和進階網路釣魚。不同於透過掃描檔案尋找已知特徵碼的傳統防病毒解決方案，下一代防病毒解決方案採用全觀式做法，檢查每一個在終端上運作的流程，並利用 AI 和 ML 智慧偵測及主動防堵以往未知的惡意軟體形式。

³ 2018 年終端安全風險現狀, Ponemon Institute



**防病毒/
下一代防病毒**

運用多種技術防止
惡意軟體感染



特權管理

管理本機管理員權限，
同時維持用戶生產力

要素三： 特權管理解決方案

終端特權管理解決方案可幫助您解決與特權帳戶（例如 Windows 或 Mac 管理員帳戶）相關的風險。特權帳戶用於控制檔案、目錄、服務及用戶存取權限，如果落入惡人手中，就可能被用來竊取資料或破壞系統。

攻擊者經常試圖透過終端上的惡意軟體或網路釣魚攻擊獲取未經授權存取特權帳戶的權限。一旦取得立足點，他們便可橫越網路尋找高價值的目標，並使用升級的特權竊取機密資訊或破壞關鍵應用程式。Forrester 估計至少有 80% 的資料外洩與特權憑證遭受滲透有關。⁴

終端特權管理解決方案透過移除本機管理權限及根據政策嚴格控制用戶與應用程式許可來幫助降低暴露風險。

執行最小特權原則（授予用戶執行其工作所需的最小特權組合），可防止橫向移動並改善您的安全態勢，而又不會降低用戶的生產力或影響業務績效。建立應用程式控制，可防止已知惡意應用程式執行並限制未經批准的應用程式運作，從而降低風險與不確定性。

包括 [Gartner](#) 在內的產業分析機構都認為，特權存取管理是安全及風險管理領導者的優先要務。⁵ [網際網路安全中心](#)也建議以控制特權管理帳戶的使用作為 [最佳實踐做法](#)。

⁴ The Forrester Wave™：特權身份管理，2018 年第 4 季

⁵ Gartner, Smarter with Gartner, Gartner 2019 年十大安全計劃，2019 年 6 月 18 日

要素四： 應用程式修補工具及最佳實踐做法

應用程式修補工具可協助您有效追蹤及實施終端軟體更新，以加強您的安全態勢。精明的攻擊者及網路犯罪份子不斷探求可利用的應用程式安全漏洞。軟體供應商則持續發佈修補程式來解決已知漏洞。在這場持久的貓鼠遊戲中，應用程式必須保持最新狀態，才能永遠領先惡人一步。

對許多組織而言，管理應用程式更新是一項挑戰。根據一項研究指出，典型的 IT 組織平均需要 34 天修補高嚴重性的安全漏洞。⁶ 應用程式修補解決方案可幫助您摒除人工密集、易出錯且耗時的修補程式管理流程並加強網路安防準備。

大多數應用程式修補程序解決方案提供：

- 庫存掃描程式以發現分散於整個企業的所有應用程式
- 狀態儀表板及報告以識別已修補且易受攻擊的應用程式
- 自動執行修補程式批准、分發及安裝程序的工具

⁶ 生產環境 Web 應用程式安全報告，tCell by Rapid7



應用程式修補

套用應用程式更新
以解決安全問題



作業系統修補

提供作業系統級
安全錯誤修復

要素五： 作業系統修補工具及最佳實踐做法

領先的終端作業系統供應商會定期發佈軟體更新，以修復程式錯誤及解決安全問題。就像應用程式更新一樣，您需要隨時留意終端作業系統更新，以保持您的數位業務安全性。您可設定操作系統自動更新或實施其他系統與方法來減少安全漏洞，確保所有公司桌上型電腦、筆電和伺服器均執行最新版本的作業系統。

每家供應商都有各自發佈作業系統修補程式的做法，因此必須個別考量。Microsoft 在每月第二個星期二發佈 Windows 伺服器及 Windows 桌上型電腦的[安全更新](#)。您可使用 Windows Update 自動安裝這些修補程式。將更新部署至生產環境之前，如果您想要先進行測試，則可使用 Windows Server Update Services (WSUS) 或第三方應用程式修補工具按照自己的時程表發佈及實施作業系統更新。

Apple 會定期發佈 macOS 軟體（可能包括安全更新）。您可以[設定 Mac](#)以手動或自動安裝 macOS 更新。

總結

終端為當今的數位業務帶來重大安全風險。精明的攻擊者可利用終端的安全漏洞竊取機密資訊或干擾 IT 服務，進而造成收益損失及高額的監管罰款及法律和解金。針對終端安全採取縱深防禦方法（建立廣泛的終端安全控制措施），可增強您的安全態勢及降低暴露風險。

特權管理是有效終端安全策略的關鍵，但卻常被輕忽。惡意內部人員或外部攻擊者經常利用終端管理員帳戶取得網路上的立足點，然後橫向移動以滲透或破壞更高價值的目標。

終端特權管理解決方案可限制特權存取，授予用戶執行其工作所需的最小權限組合，不削弱用戶生產力而能增強安全性。終端特權管理解決方案可減少入口終端處的威脅，防止橫向移動及惡意軟體散播，進而協助您降低風險及獲取更大的數位轉型成果。

關於 CyberArk

CyberArk 是特權存取安全領域的全球領導者。特權存取管理是 IT 安全的關鍵環節，可保護整個企業、雲端及整個開發維運流程的資料、基礎設施及資產。CyberArk 提供業界最完整的解決方案，降低特權憑證及金鑰所帶來的風險。公司在防禦外部攻擊者及惡意內部人員方面深受世界一流機構組織的信任，包括過半數的財星 100 大企業。

CyberArk 終端特權管理器可讓您在終端上實行最小特權安全機制，幫助防堵及遏制威脅，並降低資訊被盜竊或加密及勒索的風險。解決方案可抵禦憑證盜竊嘗試及控制應用程式，在攻擊者取得控制權並釀成重大災害之前從入口點攔阻攻擊。CyberArk 終端特權管理器是全方位終端安全策略的重要一環，用於保護 Windows Server、Windows PC 和 Mac，並可作為軟體即服務解決方案輕鬆、快速部署。

[詳細瞭解資訊](#)

© 2020 CYBERARK SOFTWARE LTD 版權所有。保留一切權利。本出版品僅作為參考資訊之用且依「現狀」提供，不含任何明示或暗示性保證，包括對適銷性、任何特定目的之適用性、非侵權性或其他任何方面的保證。在任何情況下，CYBERARK 均無需對任何損害承擔責任，尤其對於任何直接、特殊、間接、繼發或偶發的損害，或因使用或依賴本出版品而產生的利潤損失、收入損失或使用損失、替換商品的成本、資料損失或損壞，CYBERARK 概不承擔任何責任，即使 CYBERARK 已被告知可能發生該等損害。

03.20.Doc.50320